PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)	
	)	
Kouznetsov et al.	)	Group Art Unit: 2141
	)	
Application No. 10/057,709	)	Examiner: Taylor, Nicholas R.
	)	
Filed: January 25, 2002	)	
	)	
For: SYSTEM AND METHOD FOR PROVIDING WEB BROWSER-BASED SECURE REMOTE NETWORK APPLIANCE CONFIGURATION ON A DISTRIBUTED COMPUTING ENVIRONMENT	)	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION OF PRIOR INVENTION IN THE UNITED STATES OR IN A NAFTA OR WTO MEMBER COUNTRY TO OVERCOME CITED PATENT OR PUBLICATION (37 C.F.R. section 1.131)

PURPOSE OF DECLARATION

1. This declaration is to establish completion of the invention in this application in the United States at a date prior to June 25, 2001, which is the effective date of United States Patent Publication No. 2002/0198969 that was cited by the Examiner.

2. The person making this declaration is an inventor, Victor Kouznetsov.

FACTS AND DOCUMENTARY EVIDENCE

3. To establish the date of completion of the invention of this application, the following statement and exhibit are submitted as evidence:

EXHIBIT A– Confidential disclosure document and an e-mail referring to the confidential disclosure document generated before the filing of the present patent application showing the conception and/or reduction of practice of a framework for network appliance management in a distributed computing environment at least as early as April 3, 2001. See attached.

STATEMENT: I, Victor Kouznetsov, hereby state that the invention in the above patent application was conceived and/or reduced to practice at a date prior to June 25, 2001, as evidenced, at least in part, by EXHIBIT A. In particular, at a date prior to June 25, 2001, the invention in the above patent application was at least conceived to include one or more network appliances interconnected within a bounded network domain defined by a common network address space; and a configuration client comprising an applet executing within a Web browser and configuring the network appliances, comprising: a status module broadcasting a query message to the network appliances and processing a

response message containing network settings, including a physical network address, received by the applet from at least one such network appliance responsive to the query message; and a configuration module generating and sending a configuration packet using the physical network address for each at least one such network appliance sending a response message and requiring configuration.

Moreover, the invention in the above patent application was conceived to include at least one network appliance sending a response message containing network settings responsive to a query message broadcast over a specified network domain within which the at least one network appliance operates; a configuration client generating a configuration package for the at least one network appliance and containing centrally managed network settings customized for the at least one network appliance; and a bootstrap module on the at least one network appliance installing the configuration package as part of an initialization bootstrap operation, as well as other claimed features, as well as other claimed features.

From this statement and attached exhibit, it is clear that the invention in this application was made at a date prior to June 25, 2001.

DILIGENCE

4. It is hereby declared that applicant acted diligently from a time prior to the effective date of United States Patent Publication No. 2002/0198969 up to reduction to practice or the filing of the above application.

TIME OF PRESENTATION OF THE DECLARATION

5. This declaration is submitted prior to a final rejection or with a first reply or after a final rejection for the purpose of overcoming a new ground of rejection or requirement made in such final rejection. Thus, the declaration submitted herewith is considered timely and should be considered. See MPEP 715.09 (C).

DECLARATION

6. As a person signing below:

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURE(S)

Inventor's signature:  Victor Kouznetsov Date: 6/21/05

Country of Citizenship: USA

Residence: USA

Hamaty, Christopher

From: Patrick Inouye [pjs_inouye@earthlink.net]
Sent: Thursday, April 26, 2001 12:12 PM
To: Christopher Hamaty
Subject: New disclosures

Disclosure Memo Apr 2001.pdf (...

Chris,

Per my meeting with Victor on 4/3/01, I obtained the following disclosures.

Best regards,
Patrick

MEMORANDUM

To: Christopher J. Hamaty, Esq.
Network Associates, Inc.

From: Patrick J.S. Inouye

Date: April 24, 2001

Re: New Invention Disclosures

Docket No.: 002.0002.01

During my meeting at Network Associates' Beaverton, Oregon office on April 3, 2001, I met with Victor Kouznetsov and colleagues, and obtained the following invention disclosures:

1. Secure Remote Configuration Network Appliances Using Web-Based Administration

Inventors: Victor Kouznetsov, Dan Melchione, Michael Pak, and Nick Hogle

Conception: May-June 2000

Disclosure: March 2001 (beta testing)

Background: Network appliances are gaining increasingly widespread usage. These devices include firewall, storage, printer and server-type devices. Each requires configuration and administration.

Solution: The invention is directed to providing a web-based solution to administering and configuring network appliances. The following procedure is followed:

1. Plug network appliance into a network as a customer.
2. Connect to a Web portal.
3. Credential the network appliance.
4. Receive applets into the network appliance. Note: the applets are able to self-configure a non-configured network appliance.
5. Run a browser application in a client on the network.

Using the browser, a user can "talk" to the network appliance. A sequence of broadcast messages is used to configure the network appliance.

In the preferred embodiment, the configuration is performed in a secure manner. Once configured, the network appliance requests signed packets from the server.

In a further embodiment, the client browser can be used to configure the network appliance. First, a signed applet is broadcast to the network appliance, using a media access controller (MAC) address. Alternatively, the network appliance can directly request packets from the portal.

Note that two digital signatures, including date and time stamps, are required to prevent replay attacks.

Prior art: DHCP devices offer a similar form of configuration of network appliances. However, DHCP uses push technology and lacks the security provided by digital signatures.

2. Secure Network Appliance Management Framework

Inventors: Victor Kouznetsov, Michael Pak, Dan Melchione, Ian Shaughnessey

Conception: August 2000

Disclosure: August 2000

Background: The population of components of a network, including network appliances, can change over time. Maintaining the configuration and currency of the software and configurations is complicated by a dynamically changing environment.

Solution: A secure beat (SB) is communicated from the network appliances to the configuration server. The network appliances and peer network devices must be HTTP or HTTPS compliant. A list of components is periodically pulled by each appliance and compared. Static components, that is, components shared with other users, such as *.dat* files and dynamic components, that is, components maintained in the client space, are updated and patched as necessary.

Operationally, each network appliance registers at a server component website. The secure beat is periodically sent out to the central server. Missing a "beat" will generate an event at the server. Each network appliance will periodically upload and download information as needed to maintain the status of virus scanning software, package updates, and configuration information.

Note: the framework does not require a "hole" in the firewall. Remote configurations, installations and updates are received in a secure manner and fed back to the central repository for reporting purposes. Thus, network appliances are converted into configuration delivery platforms, allowing secure provisioning of systems for network appliances.

Prior art: None.

3. **Dynamic Parsing of Transient Messages**

Inventors: Davide Libenzi

Conceived: December 2000

Disclosure: December 2000

Background: The same electronic mail messages are often circulated among many different users within a single enterprise computing environment. Ideally, each user will have anti-virus protection measures in force. However, a high degree of duplication occurs due to redundant scanning by each of the users of the same identical electronic mail messages.

Solution: A virus screening system is introduced at the network application gateway. The virus screen provides SMTP-compliant content filtering. A decision on whether to accept or reject an e-mail message is made as the e-mail is transmitted. For instance, the subject line is typically received before the body of the message. Virus screening rules can be applied as the message is received, thereby dramatically reducing the number of messages received in toto.

Network appliances can also provide virus screening. An incoming message stream can be prefiltered and anti-virus rules applied in a like manner.

Prior art: None.

4. **Efficient Virus Scanning of Transient Messages Using Dynamically Cacheable Digests**

Inventors: Dan Melchione and Davide Libenzi

Conceived: April 3, 2001

Disclosure: None

Background: This invention builds on the previous invention by further streamlining the virus screening process.

Solution: An index table of scanned e-mail is created. As new messages are received, the location of the message is stored and a cryptohash of the information, or a subset, such as the header, is pulled as a digest. Consequently, virus screening of subsequent messages uses the cryptohash digest in lieu of the message, thereby enabling rapid detection of duplicate messages.

Prior art: None.

5. **Selectively Applying Message Digests of Infectible Message Parts for Efficiently and Dynamically Performing Virus Scanning**

Inventor: Dan Melchione

Conceived: April 3, 2001

Disclosure: None

Background: See #4 above.

Solution: The system maintains a parse tree of infectable parts of e-mail messages. The parse tree contains headers, bodies and attachments as necessary, preferably using MIME encoding. The parse tree is cached, thereby saving time and avoiding duplicative work to scan messages over.

The system performs a selective comparison of messages and only compares those parts which are infectable. This approach saves time with forwarded messages where an attachment need not be rescanned.

Prior art: None.

6. **File-Based Mail Store Indexed Using Hashed Filenames**

Inventor: David Libenzi

Conceived: October 2000

Disclosure: December 2000

Background: The storage of electronic mail messages is generally based on the file system upon which the mail service operates. Certain file systems, such as the EST-2 file system under the Linux operating system, is inefficient when handling large directories. Moreover, large directories and deep subdirectory trees are often non-portable and cannot be used by gateway systems.

Solution: The performance of mail service can be optimized by creating a hash table of messages. Preferably, the hash table uses a double-prime-+2 methodology, whereby a message filename is hashed to determine a subdirectory in which to store the message. This approach creates a portable solution and allows messages to be recovered in an expedient manner.

Prior art: None.

7. **Application Service Delivery Architecture**

Inventors: Victor Kouznetsov, Michael Pak, and Dan Melchione

Conception: May 2000

Disclosure: March 2001 (beta testing)

Background: As network appliances become increasingly ubiquitous, these devices offer an opportunity to deliver services directly to end-users.

Solution: Network appliances can be augmented to deliver functionality and ongoing services to end-users. This approach represents the automation of the virtual personal network concept in which end appliances provide subscription monitoring update configuration services in a closed loop format. The paradigm is to use web service to deliver provisioning, web browsers to deliver ubiquitous information access, and network appliances top deliver applications.

Prior art: None.